

### CLAIMS

1. A data processing system comprising a first arithmetic unit comprising at least one finite field multiplier and at least one finite field adder for  
5 selectively performing at least two finite field arithmetic calculations; the data processing system comprising means to use a previous finite field arithmetic calculation result of the first arithmetic unit in a current finite field arithmetic  
10 calculation of the first arithmetic unit to determine respective coefficients of at least part of at least a first polynomial.
2. A data processing system as claimed in claim 1 in which a first arithmetic operation of the at least  
15 two arithmetic operations comprises a first finite field multiplication operation.
3. A data processing system as claimed in claim 2 in which the first finite field multiplication operation comprises calculating at least a first  
20 multiplication of  $\delta\sigma^{(i-1)}(x)$  in a first clock cycle.
4. A data processing system as claimed in claim 2 in which the finite field arithmetic operation comprises calculating at least a second  
25 multiplication operation of  $\Delta^{(i)}x\lambda^{(i-1)}(x)$  in a second clock cycle.
5. A data processing system as claimed in claim 1 in which a second arithmetic operation of the at least two arithmetic operations comprises a finite field addition operation.
- 30 6. A data processing system as claimed in claim 5 in which the finite arithmetic addition operation comprises calculating at least part of  $\delta\sigma^{(i-1)}$

$\lambda^{(i)}(x) + \Delta^{(i)} x \lambda^{(i-1)}(x)$  as the current finite field arithmetic operation using  $\delta \sigma^{(i-1)}(x)$  as at least part of the previous finite field arithmetic operation.

7. A data processing system as claimed in claim 1 further comprising at least one further such arithmetic unit operable substantially in parallel with the first arithmetic unit to calculate respective coefficients of at least part of at least a first polynomial.

8. A data processing system as claimed in claim 7 in which the first polynomial comprises at least  $\delta \sigma^{(i-1)}(x) + \Delta^{(i)} x \lambda^{(i-1)}(x)$ .

9. A data processing system as claimed in claim 1 in which the at least two arithmetic calculations comprises a second finite field multiplication operation in a third clock cycle.

10. A data processing system as claimed in claim 9 in which the second finite field multiplication operation comprises calculating at least one coefficient of a second polynomial.

11. A data processing system as claimed in claim 9 in which the second arithmetic operation comprises calculating at least  $S_{i-j+1} \sigma_j^{(i)}$ .

12. A data processing system as claimed in claim 11 in which the second arithmetic operation comprises calculating at least part of  $\Delta^{(i+1)} = S_{i+1} \sigma_0^{(i)} + S_i \sigma_1^{(i)} + \dots + S_{i-t+1} \sigma_t^{(i)}$ .

13. A data processing system as claimed in claim 1 comprising at least  $(t+1)$  such arithmetic units operable substantially in parallel, each unit producing respective coefficients of at least one of

a first polynomial,  $\sigma^{(i)}(x) = \delta \sigma^{(i-1)}(x) + \Delta^{(i)} x \lambda^{(i-1)}(x)$ , and  
 a second polynomial,  $\Delta^{(i+1)} = S_{i+1} \sigma_0^{(i)} + S_i \sigma_1^{(i)} + \dots + S_{i-t+1} \sigma_t^{(i)}$ .

14. A data processing system as claimed in claim 1 in  
 which the first arithmetic unit is arranged to  
 5 calculate at least a respective part of at least  
 part of a further polynomial.

15. A data processing system as claimed in claim 14 in  
 which the further polynomial is an error evaluator  
 polynomial.

10 16. A data processing system as claimed in claim 14 in  
 which the further polynomial comprises calculating

$$\begin{aligned}\Omega(x) &= S(x) \sigma(x) \bmod x^{2t} \\ &= (S_0 + S_1 x + \dots + S_{2t-1} x^{2t-1}) \cdot (\sigma_0 + \sigma_1 x + \dots + \sigma_t x^t) \bmod x^{2t} \\ &= \Omega_0 + \Omega_1 x + \dots + \Omega_{t-1} x^{t-1}, \text{ where}\end{aligned}$$

15  $\Omega_i = S_i \sigma_0 + S_{i-1} \sigma_1 + \dots + S_{i-t+1} \sigma_{t-1}$ , where  $i=0, 1, \dots, t-1$ .

17. A data processing system as claimed in claim 14 in  
 which the at least a respective part of at least  
 part of the further polynomial comprises  
 20 calculating:

$$\begin{aligned}\Omega_i^{(j)} &= S_i \sigma_0, \text{ for } j=0; \text{ and} \\ \Omega_i^{(j)} &= \Omega_i^{(j-1)} + S_{i-j} \sigma_j, \text{ for } 1 \leq j \leq i.\end{aligned}$$

18. A Berlekamp-Massey algorithm processing unit  
 25 comprising  $(t+1)$  finite field multipliers.

19. A Berlekamp-Massey processing element comprising  
 $(t+1)$  finite field processing units arranged, in a  
 feedback arrangement, to perform at least  $(t+1)$   
 parallel operations; each parallel operation  
 30 comprising at least two serial operations.

20. A Berlekamp-Massey algorithm having an area-latency  
 product of  $7t^2 + 7t$ .